Information Disclosure Vulnerability in Data Transfer Security Function on GT Designer3, GOT2000 Series, GOT SIMPLE Series and GT SoftGOT2000

Release date: August 3, 2023
Mitsubishi Electric Corporation

■Overview

Information disclosure vulnerability exists in the Data Transfer Security function on GT Designer3, GOT2000 Series, GOT SIMPLE Series and GT SoftGOT2000. This vulnerability allows an attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords. (CVE-2023-0525)

■CVSS[1]

CVE-2023-0525 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score:7.5

■Affected products

Affected when either of the following cases.

1. The case of transferring data with GT Designer3 Version1(GOT2000) listed in Table 1 and GOT2000 Series or GOT SIMPLE Series listed in Table2 with the Data Transfer Security function[*1] enabled.
2. The case of transferring data by the SoftGOT-GOT link function[*2] with GT SoftGOT2000 described in Table 1 and GOT2000 series described in Table 2 with the Data Transfer Security function[*1] enabled.

*1: GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG)
"5.2.10 Configuring the security setting for transferring data ([Data Transfer Security])

*2: GT SoftGOT2000 Version1 Operating Manual (SH-081201ENG)
"4.14 SoftGOT-GOT Link Function

Table 1 Affected Software

Product	Model	Affected Software versions
GT Designer3 Version1 (GOT2000)	-	1.295H and prior
GT SoftGOT2000	-	1.295H and prior

Table 2 Affected HMI Products

Series	Model	Affected Base System Application versions
GOT2000	GT27 model	01.49.000 and prior
	GT25 model	01.49.000 and prior
	GT23 model	01.49.000 and prior
	GT21 model	01.49.000 and prior
GOT SIMPLE	GS25 model	01.49.000 and prior
	GS21 model	01.49.000 and prior

<How to check the versions in use>

For how to check the versions in use, please refer to the following manual. The latest version of manual is available from MITSUBISHI ELECTRIC FA Global Website (https://www.mitsubishielectric.com/fa).

[For GT Designer3]
GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG)
"2. CREATING A PROJECT" - "■13 Help"

[For GT27/GT25/GT23/GS25 models]
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"6.9 Package Data Management" - "Property operation"

[For GT21/GS21 models]
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"15.2 OS information"

[1] https://www.first.org/cvss/v3.1/specification-document

[For GT SoftGOT2000]

GT SoftGOT2000 Version1 Operating Manual (SH-081201ENG)
"2.7 Help" – "Confirming GT SoftGOT2000 version (When [About GT SoftGOT2000...] is selected)"

■Description

Information disclosure vulnerability due to Weak Encoding for Password (CWE-261)[2] exists in the Data Transfer Security function on GT Designer3, GOT2000 Series, GOT SIMPLE Series and GT SoftGOT2000. (CVE-2023-0525)

■Impact

The vulnerability could allow an attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords.

■Countermeasures

Please carry out mitigations/workarounds below.

■Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability:

・Please follow the update steps described below to update to the mitigated version.
For the update steps, please refer to [Update steps] on the next page.
The mitigated versions are as follows.

Product	Model	Software versions
GT Designer3	–	1.300N or later

(The mitigated versions for the following products are shipped with GT Designer3 Version1(GOT2000) Ver. 1.300 N or later)

Series	Model	Base System Application versions
GOT2000	GT27 model	01.50.000 or later
	GT25 model	01.50.000 or later
	GT23 model	01.50.000 or later
	GT21 model	01.50.000 or later
GOT SIMPLE	GS25 model	01.50.000 or later
	GS21 model	01.50.000 or later

Product	Model	Software versions
GT SoftGOT2000	–	1.300N or later

・Please encrypt the communication path to the affected product with a VPN or other means.
・When Internet access is required, use a virtual private network (VPN) or other means to prevent unauthorized access.
・Use the affected products within a LAN and block access from untrusted networks and hosts.
・Prevent physical access to the network to which the product is connected.
・Install antivirus software on your personal computer that can access the affected product.
・Use the IP filter function*3 to restrict the accessible IP addresses.
*3: GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG). "5.4.3 Setting the IP filter"

[2] https://cwe.mitre.org/data/definitions/261.html

<Update steps>

[For GT Desinger3]

1. Download the latest version of GT Desinger3 Version1(GOT2000) and install on a personal computer.
   Please contact your local Mitsubishi Electric representative about GT Designer3 Version1(GOT2000).
2. Refer to the <How to check the versions in use> and check that the software has been updated to the mitigated versions.

[For GT27/GT25/GT23/GT21/GS25/GS21 models]

1. Download the latest version of GT Designer3 Version1 (GOT2000) and install on a personal computer.
   Please contact your local Mitsubishi Electric representative for GT Designer3 Version1 (GOT2000).
2. Start the GT Designer3 Version1 (GOT2000) and open the project data used in affected products.
3. Select [Write to GOT] from [Communication] menu to write the required package data to the GOT.
   Please refer to the GT Designer3 Version1 (GOT2000) Screen Design Manual (SH-081220ENG).
   "4. COMMUNICATING WITH GOT"
   The latest version of manual is available from MITSUBISHI ELECTRIC FA Global Website (https://www.mitsubishielectric.com/fa).
4. After writing the required package data to the GOT, refer to the <How to check the versions in use> and check that the software has been updated to the mitigated versions.

[For GT SoftGOT2000]

1. Download the latest version of GT SoftGOT2000 Version1 and install on a personal computer.
   Please contact your local Mitsubishi Electric representative about GT SoftGOT2000 Version1.
2. Refer to the <How to check the versions in use> and check that the software has been updated to the mitigated versions.

■Acknowledgement

Mitsubishi Electric would like to thank JINYOUNG KIM, JEONGHOON BAE, YIJOON JUNG, and HYEOKJONG YUN of "ot vulnerability" who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html